PRAXIS
RES JUDICATA

Легализация «массовой слежки» Европейским Судом по правам человека: что стоит за постановлением по делу *Биг Бразер Вотч и другие против Соединённого Королевства*?

Вера Русинова*

13 сентября 2018 года ЕСПЧ вынес постановление по делу *Биг Бразер Вотч*, в котором он проверял на соответствие Конвенции правовые акты Соединённого Королевства, регулирующие массовый перехват сообщений и их метаданных, а также правовой режим обмена полученной информацией со спецслужбами других государств. Использовав подход, заключающийся в том, что при принятии решения о введении режима массового перехвата данных государства пользуются широкой дискрецией, но при этом дискреция при использовании этого режима гораздо у́же и должна удовлетворять набору критериев, которые нацелены на то, чтобы минимизировать риск злоупотребления властью, Суд тем самым легализовал использование этой меры государствами – членами Совета Европы. При оценке того, что содержательно стоит за признанием ЕСПЧ «массовой слежки» *per se* не нарушающей Конвенцию, в статье демонстрируется, что Суд, действуя как эксплицитно, так и имплицитно, изъял ряд ключевых параметров этих мер из-под теста проверки на «законность», «необходимость в демократическом обществе» и «пропорциональность» и существенно снизил планку требований в отношении остальных составляющих режима массового перехвата данных. Это является явным разворотом от начавшего кристаллизоваться несколько лет назад благодаря деятельности самого ЕСПЧ и Суда ЕС достаточно прогрессивного подхода к защите права на уважение частной жизни и защиту персональных данных в условиях всё увеличивающихся аппетитов государств к массовому сбору информации. Статья завершается размышлениями о том, какие политические основания могли оказать влияние при применении ЕСПЧ метода «балансирования», предопределив трактовку того, что является «необходимым в демократическом обществе».

DOI: 10.21128/2226-2059-2018-4-3-20

🗝 *Право на уважение частной жизни; частная жизнь; массовая слежка; метаданные; Европейский Суд по правам человека; Суд Европейского Союза*

1. Введение

Массовая слежка *per se* не нарушает Конвенцию о защите прав человека и основных свобод (*далее* – Конвенция): «решение о введении режима массового перехвата для того, чтобы идентифицировать тем самым неизвестные угрозы национальной безопасности», подпадает под широкие пределы усмотрения, которые есть у государств при выборе того, как лучше достигнуть легитимную цель по защите безопасности. Это не выдержка из

* *Русинова Вера Николаевна* – доктор юридических наук, LL.M (Göttingen), профессор департамента общих и межотраслевых юридических дисциплин факультета права Национального исследовательского университета «Высшая школа экономики», Москва, Россия (e-mail: vrusinova@hse.ru). Статья подготовлена в результате проведения исследования (проект № 17-01-0042) в рамках Программы «Научный фонд Национального исследовательского университета "Высшая школа экономики" (НИУ ВШЭ)» в 2017–2018 годах и в рамках государственной поддержки ведущих университетов Российской Федерации «5-100».

решения Европейского Суда по правам человека (*далее* — ЕСПЧ; Суд) по делу *Вебер и Саравия против Германии*[1], принятого в 2006 году на «заре» становления технических возможностей по перехвату, хранению и обработке массовых данных и до разоблачений Эдварда Сноудена, продемонстрировавших, насколько интенсивно государства используют инструментарий по массовому перехвату сообщений, персональной информации, а также «метаданных»[2] и насколько уязвима система их защиты. Нет, это квинтэссенция совсем недавно вынесенного ЕСПЧ постановления по делу с «говорящим» названием *Биг Бразер Вотч и другие против Соединённого Королевства*[3].

В первую очередь именно из-за этого вывода о допустимости массового перехвата данных *per se*, несмотря на то что Суд, казалось бы, встал на сторону заявителей, признав, что законодательство Соединённого Королевства по ряду аспектов нарушает право на уважение частной жизни, а также свободу выражения (статьи 8 и 10 Конвенции), это решение оценивается комментаторами как «частичная»[4] или даже «пиррова победа»[5] права на частную жизнь над «массовой слежкой». Данное постановление ещё может быть пересмотрено Большой Палатой, но тот факт, что в этой части оно повторяет составленное другой палатой ЕСПЧ тремя месяцами ранее постановление по делу *Центрум фёр Рэттвиса против Швеции*[6] и ни один из судей, выразивших особое или несовпадающее мнение, не поставил этот вывод под сомнение[7], вполне может свидетельствовать о том, что ЕСПЧ определился с подходом к разрешению дел о проверке на соответствие Конвенции правовых актов, регулирующих массовый перехват содержания сообщений и их метаданных.

Отсюда возникает потребность в том, чтобы разобраться, действительно ли этот подход по, наверное, одному из самых принципиальных вопросов, связанных с «массовой слежкой», вытекает из сложившейся практики самого ЕСПЧ и как он соотносится с позицией также занимающегося вопросами защиты права на защиту частной жизни и персональных данных Суда Европейского Союза (*далее* — Суд ЕС), так как более половины членов Совета Европы участвуют в этой международной организации. Оценивать значение признания ЕСПЧ «массовой слежки» *per se* не нарушающей Конвенцию можно, только установив, что содержательно за этим стоит в плане защиты права на уважение частной жизни: в какой части Суд отказался от оценки принимаемых государствами мер на соответствие статье 8, а в какой усилил или, наоборот, ослабил уже применявшиеся им критерии. Наконец, логично встаёт вопрос о том, что повлияло или могло повлиять на мнение судей при выборе парадигмы рассмотрения дел, связанных с «массовой слежкой», и существовала ли у Суда возможность вынести иной вердикт. Настоящая статья, являясь одним из первых откликов на постановление по делу *Биг Бразер Вотч*, ограничивается анализом именно этих аспектов, остав-

[1] European Court of Human Rights (*далее* — ECtHR). *Weber and Saravia v. Germany*. Application no. 54934/00. Decision on Admissibility of 29 June 2006.

[2] Понятие «*метаданные*» используется в настоящей статье в значении «данные о других данных», то есть «все данные, которые не являются содержанием сообщения». См.: European Commission for Democracy through Law (Venice Commission). Report on the Democratic Oversight of Signals Intelligence Agencies. 20–21 March 2015. § 2. URL: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-e (дата обращения: 16.11.2018) (*далее* — Venice Commission. Report of 2015).

[3] ECtHR. *Big Brother Watch and Others v. the United Kingdom*. Applications nos. 58170/13, 62322/14 and 24960/15. Judgment of 13 September 2018. § 314 (*далее* — *Big Brother Watch v. UK*).

[4] См.: *Milanovic M.* ECtHR Judgment in Big Brother Watch v. UK // EJIL: Talk! 2018. 17 September. URL: https://www.ejiltalk.org/ecthr-judgment-in-big-brother-watch-v-uk/ (дата обращения: 16.11.2018); *Tzanou M.* Big Brother Watch and Others v. the United Kingdom: A Victory of Human Rights over Modern Digital Surveillance? // Verfassungsblog. 2018. 18 September. URL: https://verfassungsblog.de/big-brother-watch-and-others-v-the-united-kingdom-a-victory-of-human-rights-over-modern-digital-surveillance/ (дата обращения: 16.11.2018).

[5] См.: *Christakis Th.* A Fragmentation of EU/ECHR Law on Mass Surveillance: Initial Thoughts on the Big Brother Watch Judgment // European Law Blog. 2018. 20 September. URL: http://europeanlawblog.eu/2018/09/20/a-fragmentation-of-eu-echr-law-on-mass-surveillance-initial-thoughts-on-the-big-brother-watch-judgment/ (дата обращения: 16.11.2018).

[6] ECtHR. *Centrum för Rättvisa v. Sweden*. Application no. 35252/08. Judgment of 19 June 2018. § 112. См. также: *Lubin A.* Legitimizing Foreign Mass Surveillance in the European Court of Human Rights // Just Security. 2018. 2 August. URL: https://www.justsecurity.org/59923/legitimizing-foreign-mass-surveillance-european-court-human-rights/ (дата обращения: 16.11.2018). По состоянию на 27 ноября 2018 года запрос о пересмотре этого решения Большой Палатой ЕСПЧ всё ещё находится на рассмотрении.

[7] См.: *Big Brother Watch v. UK*. Partly Concurring, Partly Dissenting Opinion of Judge Koskelo, Joined by Judge Turkovic; Joint Partly Dissenting and Partly Concurring Opinion of Judges Pardalos and Eicke.

ляя в качестве поля для будущих научных изысканий обширнейший список проблем и вопросов, возникающих в связи с принятием данного решения.

2. Становление прогрессивного подхода к оценке правомерности «массовой слежки»

2.1. Европейский Суд по правам человека

Постановления по делу *Центрум фёр Рэттвиса* и *Биг Бразер Вотч* не являются первыми, вынесенными после *Вебер и Саравия*, решениями, в которых ЕСПЧ обратился к проблеме «массовой слежки» как мере, предпринимаемой в рамках борьбы с терроризмом или защиты государственной безопасности. Для того чтобы отследить эту практику и выяснить, насколько факты двух рассмотренных в 2018 году дел отличаются от предыдущих решений, важно определиться с тем, что понимается под данным понятием. Термин «массовая слежка» не является правовым и используется для характеристики размаха мер по сбору данных. Отсюда «массовая слежка» может применяться в рамках как уголовно-правовой парадигмы — при расследовании преступлений, поиске пропавших лиц, так и парадигмы, связанной с добычей разведывательных данных в рамках защиты государственной (или национальной) безопасности. При этом следует отметить, что граница между этими парадигмами становится достаточно условной, когда речь идёт о борьбе с терроризмом. Массовая слежка может быть как общей, когда перехватываются все сообщения, так и целенаправленной, когда круг лиц, чьи коммуникации перехватываются, не является достаточно определённым или обозначен слишком широко[8]. Меры по массовому перехвату данных могут быть нацелены только на иностранных граждан, или же на коммуникации с участием иностранных граждан, или быть неизбирательными. Наконец, «массовая слежка» может применяться не только государством, но и компаниями, то есть быть как правительственной, так и корпоративной.

Условной точкой отсчёта, когда в ЕСПЧ стал складываться подход к оценке массового перехвата данных, следует считать принятое в 2006 году решение о приемлемости по делу *Вебер и Саравия против Германии*. В этом решении Суд проверял на соответствие Конвенции законодательство о «стратегическом мониторинге», позволявшее перехватывать телекоммуникации для целей выявления и предотвращения таких опасностей, как совершение вооружённого нападения на ФРГ или террористического акта, то есть оценивал установление слежки не в качестве целенаправленной, а в качестве общей меры[9]. Хотя ЕСПЧ не нашёл оснований считать «массовую слежку» нарушающей статью 8 и признал жалобу явно необоснованной, он суммировал критерии, которые должны применяться для оценки предсказуемости правовой базы, регулирующей тайную слежку[10].

Сделанные в решении по делу *Вебер и Саравия* выводы были подтверждены в 2008 году в деле *Либерти и другие против Соединённого Королевства*, в котором ЕСПЧ рассматривал ситуацию, связанную с осуществлённым Министерством обороны в 1990-е годы массовым перехватом телефонных переговоров, факсимильных сообщений и электронной почты, которые передавались с помощью микроволновых радиосигналов между двумя станциями «Бритиш Телеком»[11]. В этом решении Суд прямо подчеркнул, что «не существует каких-либо оснований для того, чтобы применять иные принципы, касающиеся доступности и понятности правил, которые касаются перехвата индивидуальных сообщений, с одной стороны, и более общих программ слежки — с другой»[12].

Однако в обоих делах — в *Вебер и Саравия*, а также в *Либерти и других* — ЕСПЧ не упоминал в качестве критерия наличие подозрения, тем самым допуская предельно общий перехват данных. Этот критерий применялся Судом только в отношении использования тайной слежки в рамках уголовно-правовой парадигмы[13]. Ситуация изменилась

[8] См.: Venice Commission. Report of 2015. § 64.

[9] См.: *Weber and Saravia v. Germany*. § 4.

[10] См.: Ibid. § 95.

[11] См.: ECtHR. *Liberty and Others v. the United Kingdom*. Application no. 58243/00. Judgment of 1 July 2008.

[12] Ibid. § 63.

[13] См.: ECtHR: *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*. Application no. 62540/00. Judgment of 28 June 2007. § 79, 80; *Iordachi and Others v. Moldova*. Application no. 25198/02. Judgment of 10 February 2009. § 51.

с вынесением Большой Палатой 4 декабря 2015 года постановления по делу *Роман Захаров против России*, в котором Суд проанализировал российское законодательство, уполномочивающее правоохранительные органы и спецслужбы на прослушивание телефонных переговоров. Являясь председателем регионального отделения «Фонда защиты гласности», заявитель полагал, что его звонки перехватываются, так как операторы мобильной связи установили оборудование, которое позволяет спецслужбам прослушивать все телефонные переговоры[14]. В связи с тем, что российское законодательство об оперативно-розыскной деятельности в качестве оснований для применения прослушивания телефонных переговоров указывало, среди прочего, сведения о «событиях или действиях (бездействии), создающих угрозу государственной, военной, экономической, информационной или экологической безопасности Российской Федерации»[15], Суд не ограничивал проверку исключительно уголовно-правовой парадигмой, связанной с расследованием конкретных преступлений. Признавая, что при принятии мер в рамках защиты национальной безопасности соблюдение принципа «предсказуемости» не заходит так далеко, чтобы требовать существования правовых норм, перечисляющих в деталях, какое поведение может послужить основанием для введения тайной слежки, ЕСПЧ тем не менее подчеркнул, что подобная формулировка — а надо отметить, что это понятие нигде не расшифровывалось — оставляет властям «практически неограниченную дискрецию», открывающую широкие возможности для злоупотребления[16].

Важно, что при рассмотрении вопроса об уполномочивании на проведение прослушивания Суд вышел на применимость стандарта «обоснованного подозрения» не только в отношении планирования или совершения преступлений, но и других деяний, которые могут явиться основанием для установления прослушивания, прямо указав на «действия, угрожающие национальной безопасности»[17]. ЕСПЧ выявил, что сфера судебного контроля была ограничена: не имея доступа к соответствующим материалам, российские суды были не в состоянии проверить, действительно ли имелся «существенный фактический базис», чтобы подозревать лицо, в отношении которого устанавливалось прослушивание[18]. В результате ЕСПЧ раскритиковал практику, когда суды выносили постановления о перехвате телефонных переговоров без упоминания конкретных лиц или номеров телефонов, которые должны прослушиваться, или уполномочивали на применение этой меры в отношении всех телефонных переговоров в районе, где было совершено преступление[19].

Пусть несколько отличающийся, но в основе своей сопоставимый подход к оценке правомерности ограничения государствами права на защиту частной жизни пронизывает и вынесенное буквально через месяц после рассмотрения жалобы Романа Захарова постановление по делу *Сабо и Висси против Венгрии*[20]. В этом деле ЕСПЧ по жалобе заявителей, которые, будучи сотрудниками оппозиционной неправительственной организации, подозревали, что могли быть подвергнуты слежке, проверял на соответствие Конвенции венгерское законодательство в той части, в которой оно предоставляет возможность применять эту меру для сбора информации в целях «предотвращения террористических актов или в интересах национальной безопасности»[21].

Несмотря на то что в проанализированных Судом правовых актах не было прямо установлено, что может применяться режим «массовой слежки», ЕСПЧ в данном решении рассматривал и эту ситуацию, поскольку норму о том, что подвергающиеся режиму перехвата данных лица могут быть идентифицированы и как «круг лиц», он растолковал как означающую, что под слежкой может оказаться любой, и в итоге этой мерой может быть охвачено большое число лиц[22]. Этот ас-

[14] См.: ECtHR. *Roman Zakharov v. Russia*. Application no. 47143/06 [GC]. Judgment of 4 December 2015. § 10.

[15] Пункт 2 статьи 7 Федерального закона «Об оперативно-розыскной деятельности» от 12 августа 1995 года № 144-ФЗ с посл. изм. и доп. // Собрание законодательства Российской Федерации. 1995. № 33. Ст. 3349.

[16] *Roman Zakharov v. Russia*. § 246–248.

[17] Ibid. § 260.

[18] Ibid. § 261–262.

[19] См.: Ibid. § 265.

[20] См. подробнее об этом постановлении: *Pásztor E.* Secret Intelligence Gathering — a Low Threshold Still Too High to Reach // ELTE Law Journal. 2017. No. 1. P. 99–112, 104–112.

[21] ECtHR. *Szabó and Vissy v. Hungary*. Application no. 37138/14. Judgment of 12 January 2016. § 7, 10–11.

[22] См.: Ibid. § 67.

пект законодательства был подвергнут Судом жёсткой критике как не соответствующий принципу «строгой необходимости». То, что властям было достаточно только сослаться на причины, обосновывающие необходимость применения данной меры, ЕСПЧ признал не соответствующим этому принципу. Суд подчеркнул, что определение круга лиц, в отношении которых устанавливается слежка, должно происходить на основании «индивидуального подозрения» при наличии соответствующих материалов или фактов[23]. «Тайная слежка может быть совместима с Конвенцией, – уточнил ЕСПЧ, – только если это строго необходимо... для получения жизненно важной информации при проведении отдельной ["*individual*". – *В.Р.*] операции», и потребовал от национальных органов власти проверять, существуют ли достаточные основания для перехвата определённых сообщений в каждом конкретном случае[24]. К гарантиям, которые должны соблюдаться при проведении таких операций, Суд причислил необходимость уполномочивания именно судебными органами, дополнив, что только «в исключительных обстоятельствах» это допустимо со стороны органов исполнительной власти, но только при условии последующего судебного контроля[25]. Кроме того, ЕСПЧ отдельно выделил необходимость уведомления лиц, подвергавшихся тайной слежке[26]. Надо признать, что наложение Судом таких строгих рамок на тайную слежку для целей получения информации, необходимой в контексте защиты государственной безопасности, практически сводило к нулю возможность использования массового перехвата данных.

О формировании в практике ЕСПЧ вектора предельно строгого отношения к покушениям на частную жизнь при проведении массовой слежки свидетельствует тот факт, что данное постановление было раскритиковано как недостаточно жёсткое из-за того, что Суд не использовал применявшийся им при рассмотрении дел, связанных с установлением слежки, стандарт «разумного подозрения» (как это было сделано Большой Палатой в деле *Романа Захарова*), предпочтя снизить планку до «индивидуального подозрения»[27]. Итак, несмотря на некоторое снижение уровня требований к характеру подозрения, в начале 2016 года ЕСПЧ всё ещё оставался сторонником допустимости только целенаправленной слежки и только при условии соблюдения целого ряда гарантий против возможных злоупотреблений со стороны властей. Это создавало уверенность в том, что в общем и целом Суд определился с вектором рассмотрения дел, связанных с массовым перехватом данных[28]. Однако, как показали решения по делам *Центрум фёр Рэттвиса* и *Биг Бразер Вотч*, эта уверенность оказалась иллюзией.

2.2. Суд Европейского Союза

Процесс оформления позиции Суда ЕС в отношении массового перехвата данных начался в 2014 году, когда был рассмотрен спор *Диджитл Райтс Ирландия*[29]. В этом деле Суд рассматривал вопрос о соответствии Хартии ЕС об основных правах Директивы 2006/24/ЕС, которая налагала на провайдеров сервисов электронных коммуникаций обязанность сохранять передаваемые через них или сгенерированные ими данные. Суд ЕС признал эту директиву недействительной, посчитав предписываемые ею меры непропорциональным вторжением в право на частную жизнь и защиту персональных данных (статьи 7, 8 и пункт 1 статьи 52 Хартии ЕС об основных правах)[30]. Ключевыми посылками, которыми руководствовался суд при оценке этого правового акта, было то, что, какой бы фундаментальной ни была цель борьбы с организованной преступностью и терроризмом, она сама по себе не оправдывает общих мер по сохранению данных; ограничения права на

[23] См.: *Szabó and Vissy v. Hungary*. § 71.
[24] Ibid. § 73.
[25] См.: Ibid. § 77, 80, 81.
[26] См.: Ibid. § 86–87.
[27] *Szabó and Vissy v. Hungary*. Concurring Opinion of Judge Pinto de Albuquerque. § 18–20.
[28] См., к примеру: *Golubok S.* Roman Zakharov v. Russia: Big Brother Under Control? // Journal for Constitutionalism and Human Rights. 2015. No. 3–4 (8). P. 20–26, 25.
[29] Court of Justice (Grand Chamber). *Requests for a preliminary ruling from the High Court of Ireland and the Verfassungsgerichtshof – Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Siochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others*. Joined Cases C-293/12 and C-594/12. Judgment of 8 April 2014 (*далее – Digital Rights Ireland*).
[30] См.: Ibid. § 69, 71.

частную жизнь и права на защиту персональных данных должны быть «*строго необходимы*» (выделено мной. — *В.Р.*)[31]. Кроме того, ссылаясь на подход ЕСПЧ, Суд ЕС исходил из необходимости существования понятных и чётких правил, регулирующих сферу применения таких ограничений и устанавливающих для затронутых лиц гарантии эффективной правовой защиты[32].

Применяя эти общие установки, Суд ЕС в первую очередь подверг критике предельно общую сферу применения обязанности по перехвату данных: из директивы следовало, что данная мера действует в отношении «всех лиц, всех видов средств электронной коммуникации, всех метаданных без какой бы то ни было дифференциации, ограничения или исключения, поставленных в зависимость от цели борьбы с серьёзными преступлениями»[33], или предотвращения угроз общественной безопасности[34]. Затем, как отметил суд, в директиве не было обозначено никаких объективных критериев, материальных или процессуальных условий, лимитирующих доступ национальных властей к этим данным, а также не было установлено необходимости проведения процедуры контроля ни судом, ни каким-либо независимым органом исполнительной власти[35]. Наконец, период предписываемого хранения данных не был поставлен в зависимость от объективного критерия, позволявшего ограничить его только тем, что строго необходимо[36].

Сделанные в решении *Диджитл Райтс Ирландия* выводы были ещё раз подтверждены и получили своё дальнейшее развитие в деле *Теле2 Свериге АБ и Вотсон* (*далее — Теле2*), решение по которому было вынесено Большой Палатой 21 декабря 2016 года. В этом деле рассматривались запросы двух судов о толковании пункта 1 статьи 15 Директивы 2002/58/ЕС в отношении защиты частной жизни и персональных данных в сфере электронных коммуникаций. Поставленные перед Судом ЕС вопросы касались того, в каком объёме выводы, сделанные Судом ЕС в деле *Диджитл Райтс Ирландия*, применимы к национальному законодательству, имплементирующему отменённую в этом решении Директиву 2006/24/ЕС. Шведский Административный апелляционный суд обратился с предварительным запросом в рамках дела, в котором оператор услуг связи «Теле2 Свериге АБ» оспаривал выданный шведским регулятором в сфере почтовых и телекоммуникационных услуг ордер о массовом перехвате данных о местоположении и трафике пользователей[37]. Второй запрос был направлен Апелляционным судом Англии и Уэльса, рассматривающим иск о соответствии праву Европейского Союза британского законодательства, регулирующего массовый перехват данных.

Повторив все выводы, сделанные ранее в деле *Диджитл Райтс Ирландия*, Суд ЕС конкретизировал, что они не означают запрета на использование государствами-участниками перехвата метаданных в качестве превентивной меры, но только при условии, что этот перехват носит не массовый, а целенаправленный характер[38] и соответствует ряду требований. Цель перехвата данных должна быть ограничена борьбой с «серьёзными преступлениями»; при выборе субъектного состава, средств коммуникаций, типов данных и времени применения данной меры должен соблюдаться принцип строгой необходимости[39]. В частности, национальное законодательство должно основываться на наличии объективных доказательств, которые способны убедить общество в наличии как минимум косвенной связи между перехватываемыми данными и борьбой с серьёзными преступлениями[40].

Принцип строгой необходимости, согласно решению по делу *Теле2*, должен соблюдаться и на стадии регулирования условий получения национальными властями доступа к перехваченным данным: ими должна преследоваться только такая цель, как борьба с

[31] *Digital Rights Ireland*. § 51, 52.
[32] См.: Ibid. § 54.
[33] Ibid. § 57.
[34] См.: Ibid. § 59.
[35] См.: Ibid. § 60–62.
[36] См.: Ibid. § 63–64.
[37] См.: Court of Justice (Grand Chamber). *Requests for a preliminary ruling under Article 267 TFEU, made by the Kammarrätten i Stockholm (Administrative Court of Appeal, Stockholm, Sweden) and the Court of Appeal (England & Wales) (Civil Division) (United Kingdom) — Tele2 Sverige AB v. Post- och telestyrelsen, and Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis*. Joined Cases C-203/15 and C-698/15. Judgment of 21 December 2016. § 2 (*далее — Tele2*).
[38] См.: Ibid. § 108.
[39] См.: Ibid.
[40] См.: Ibid. § 110.

серьёзными преступлениями[41]. Среди требований, которым должно соответствовать национальное законодательство, Суд ЕС также указал на то, что должен быть предусмотрен предварительный контроль со стороны судов или независимых органов исполнительной власти; перехваченные данные должны храниться в пределах ЕС и подлежать безвозвратному уничтожению по окончании срока хранения; подвергнутые слежке граждане должны уведомляться о проводившихся операциях и им должно быть доступно средство правовой защиты[42]. Наконец, государствам-участникам надлежит наладить надзор за соответствием национального правового режима уровню защиты, гарантированному правом ЕС[43].

Это решение, несомненно, является образчиком беспрецедентно решительного отпора попыткам снизить планку защиты частной жизни и персональных данных перед лицом появления новых технологических возможностей. Заметно также, насколько сильно оно перекликается с постановлением ЕСПЧ по делу *Роман Захаров против России*.

Вместе с тем ответ на вопрос о том, насколько решение по делу *Теле2* отправило предусматривающее массовый перехват данных законодательство государств — членов ЕС в «полный нокаут»[44], является спорным. Дело в том, что оба преюдициальных запроса, которые рассматривал в *Теле2* Суд ЕС, касались перехвата данных для целей «борьбы с преступлениями»[45] и не затрагивали таких целей, как, например, поддержание обороны или защита общественной безопасности. При этом «массовая слежка» устанавливается, как правило, вне рамок уголовно-правовой модели. С одной стороны, действительно, в тексте самой Директивы 2002/58/ЕС изпод сферы её применения выводится «деятельность, касающаяся общественной безопасности, обороны, государственной безопасности (включая экономическое благосостояние государства, когда деятельность относится к вопросам государственной безопасности), и деятельность государства в области уголовного права» и указывается, что «она не должна применяться к деятельности, которая выходит за пределы действия Договора, учреждающего Европейское сообщество» (пункт 3 статьи 1)[46]. С другой стороны, пункт 1 статьи 15 этой директивы дозволяет государствам принимать законодательные меры, которые могут ограничивать сферу применения указанных в ней прав человека и возложенных на государства обязанностей для «защиты национальной безопасности (то есть государственной безопасности), обороны, общественной безопасности и для предотвращения, расследования, обнаружения и преследования уголовно наказуемых деяний или неавторизованного использования системы электронной коммуникации». Не только истцы и ответчики, но и сами государства разошлись в мнениях относительно применимости директивы даже к случаям принятия мер, направленных на борьбу с преступлениями[47]. Рассматривая этот вопрос, Суд ЕС посчитал, что если бы эта деятельность не подпадала под действие директивы, то процитированный выше пункт 1 статьи 15 был бы лишён всякого смысла[48]. При этом суд не ограничивал свой вывод только теми мерами, которые направлены на борьбу с преступлениями, указав, что директива уполномочивает государства на принятие упомянутых в статье 15 ограничений только при условии соблюдения требований, сформулированных в этом правовом акте[49]. Таким образом, в деле *Теле2* Суд ЕС подтвердил применимость Директивы 2002/58/ЕС к мерам, связанным с защитой общественной или государственной безопасности.

Несмотря на то что решение *Теле2* посвящено только тем мерам, которые принимаются в целях борьбы с преступлениями, из текста можно вычленить общую позицию Суда ЕС и в отношении «массовой слежки», осуществляемой для иных целей. Подчёркивая, что перехват данных должен быть ограничен

[41] См.: *Tele2*. § 114, 116–119.

[42] См.: Ibid. § 120–123.

[43] См.: Ibid. § 123.

[44] *Verbruggen F.*, *Royer S.*, *Severijns H.* Reconsidering the Blanket-Data-Retention-Taboo, for Human Rights' Sake? // European Law Blog. 2018. 1 October. URL: http://europeanlawblog.eu/author/frankverbruggen/ (дата обращения: 16.11.2018).

[45] *Tele2*. § 62 et seq.

[46] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector. Article 1(3) // OJ L 201, 31.7.2002. P. 37–47. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32002L0058 (дата обращения: 16.11.2018).

[47] См.: *Tele2*. § 63, 65.

[48] См.: Ibid. § 73.

[49] См.: Ibid.

лицами, которые подозреваются в планировании или совершении серьёзного преступления или иным образом замешаны в нём, суд сформулировал: «В определённых ситуациях, когда, например, террористическая деятельность угрожает жизненно важным интересам национальной безопасности, обороны или общественной безопасности, может быть обеспечен доступ к данным *иных лиц*, если существуют объективные доказательства, из которых может быть выведено, что эти данные могут в конкретном случае внести эффективный вклад в борьбу с такой деятельностью»[50] (выделено мной. — *В.Р.*).

Конечно, следует принимать во внимание, что этот вывод относится к *obiter dictum*, однако, учитывая то, что данное решение было вынесено Большой Палатой и остаётся первым и пока единственным высказыванием Суда ЕС о массовом перехвате данных с целью защиты государственной или общественной безопасности, нельзя исключать, что он намечает вектор рассмотрения будущих дел. Среди озвученных судом ключевых положений можно перечислить: экстраординарность подобной меры, необходимость наличия объективных доказательств, а также привязку к конкретному делу.

Ряд принципиальных вопросов при этом, однако, так и остаются открытыми. Во-первых, неясно, насколько широко может быть «растянуто» использованное Судом ЕС понятие «иные лица»: может ли оно означать «все» или же привязка к объективным доказательствам, упоминание конкретного случая и подчёркивание «эффективности» вклада, который введённая мера должна иметь в деле противодействия терроризму, указывают на неприемлемость подобного сценария? Во-вторых, анализируемое высказывание Суда ЕС касается только вопроса доступа к данным, но не самого перехвата. Посвящённая же ему часть судебного решения ограничена исключительно целью борьбы с преступлениями. Высказываясь о параметрах доступа к данным и допуская расширение круга лиц до «иных», суд не мог не исходить из того, что такие данные каким-либо образом уже были перехвачены, но каким параметрам должен соответствовать такой перехват, остаётся за рамками решения по делу *Теле2*. Суд ЕС признал только, что Директива 2002/58/ЕС применима как к стадии перехвата, так и к стадии получения доступа к данным, и растолковал её положения в свете решения по делу *Диджитл Райтс Ирландия*. Однако это решение, в свою очередь, также было ограничено целью борьбы с преступлениями. Соответственно, пока можно лишь гадать, насколько жёстко Суд ЕС подойдёт к вопросу непосредственно самого перехвата данных для целей защиты государственной или общественной безопасности. В связи с тем, что на текущий момент на рассмотрении Суда ЕС находятся три преюдициальных запроса о толковании решения по делу *Теле2*[51] и они затрагивают озвученные вопросы, вскоре станет известно, в каком направлении развивается позиция этого европейского суда.

Таким образом, несколько лет назад благодаря деятельности двух судов: самого ЕСПЧ и Суда ЕС, которые в своей практике начали поступательно требовать от государств тщательного соблюдения права на частную жизнь и защиту персональных данных, начал визуализироваться достаточно прогрессивный подход к защите таких ценностей, как права человека, верховенство права и демократия в условиях возрастающей потребности государств в применении достижений технологического прогресса для защиты своей безопасности. Анализ этой практики позволяет судить о том, насколько получивший отражение в решениях по делам *Центрум фёр Рэттвиса* и *Биг Бразер Вотч* подход ЕСПЧ к соблюдению прав человека при проведении операций по массовой слежке не просто выбивается, а является разворотом от уже начавшего кристаллизоваться прогрессивного подхода.

3. Постановление ЕСПЧ по делу *Биг Бразер Вотч*: время расставаться с иллюзиями

Вынесенному ЕСПЧ 13 сентября 2018 года постановлению по делу *Биг Бразер Вотч* ещё до его оглашения была зарезервирована главная роль в практике Суда по так называемым «информационным делам». Этот про-

[50] *Tele2*. § 119.

[51] Запросы направлены судами Бельгии, Испании и Соединённого Королевства (см.: *Verbruggen F., Royer S., Severijns H.* Op. cit.).

цесс был «стратегическим» для ряда правозащитных организаций, которые стремились добиться от ЕСПЧ ужесточения подхода к оценке «массовой слежки»[52]. В этом деле, объединившем жалобы нескольких неправительственных организаций, компаний и граждан, Суд рассматривал вопрос о соответствии Конвенции трёх основных аспектов законодательства Соединённого Королевства, регулирующих применение массовой электронной слежки: перехвата сообщений, режима обмена разведывательными данными, а также сбора метаданных провайдерами телекоммуникационных услуг[53]. Цель заявителей состояла в том, чтобы убедить ЕСПЧ принять во внимание произошедший качественный скачок в технических возможностях государств по перехвату, хранению и обработке больших данных, а также учесть «фактор Сноудена».

Ожидания от дела *Биг Бразер Вотч и другие против Соединённого Королевства* оказались оправданны, по крайней мере в том смысле, что ЕСПЧ действительно вынес чрезвычайно детализированное постановление, которое, судя по всему, задаёт вектор для рассмотрения подобных жалоб в будущем и призвано снабдить правительства государств — членов Совета Европы «дорожной картой» по правовому регулированию массового перехвата данных. Именно это обстоятельство объясняет то, что данное решение практически оставило в тени другое, вынесенное тремя месяцами ранее, но несопоставимое по детализации проверки, постановление ЕСПЧ по делу *Центрум фёр Рэттвиса против Швеции*[54], которое хронологически было первым решением, в котором Суд решил отступить от уже начавшего формироваться прогрессивного подхода к оценке «массовой слежки».

Итак, в деле *Биг Бразер Вотч*, отвечая на вопрос: правомерна ли информационная массовая слежка *per se* в свете Конвенции или нет, ЕСПЧ решает отказаться от линии, намеченной в решениях по делам *Роман Захаров*, а также *Сабо и Висси*, и, основываясь на выводах, сформулированных в решении *Вебер и Саравия*, выносит поражающее своей детализированностью решение. Суть подхода, использованного Судом в деле *Центрум фёр Рэттвиса*, а затем повторённого в *Биг Бразер Вотч*, заключается в том, что при принятии решения о введении режима массового перехвата данных государства пользуются широкой дискрецией, но, соответственно, дискреция при использовании этого режима гораздо у́же и должна удовлетворять набору критериев, которые нацелены на то, чтобы минимизировать риск злоупотребления властью[55]. Скрупулёзная разработка содержания и применимости этих критериев к различным типам и этапам мероприятий по массовому перехвату данных, включая сотрудничество со спецслужбами других государств, и составляет основу постановления по делу *Биг Бразер Вотч*.

Содержательно подход ЕСПЧ к проверке соответствия режима массовой слежки Конвенции, в частности статье 8, строится на сочетании признания ЕСПЧ массового перехвата данных допустимым *per se*, что воплощается в изъятии ряда ключевых параметров этих мер из-под теста проверки на «законность», «необходимость в демократическом обществе» и «пропорциональность», с особенностями применения данного теста в отношении остальных составляющих режима. Суд выделяет четыре этапа технологии «массовой слежки»: перехват данных, фильтрацию, отбор по критериям поиска и проверку аналитиками — и по крайней мере обещает, что широкая дискреция государств по принятию решения об использовании этого режима, то есть о перехвате, будет сочетаться со строгим контролем на последующих этапах[56]. Соответственно, необходимо выяснить, что именно выводится ЕСПЧ из-под проверки и насколько строго оцениваются остающиеся параметры на самом деле.

3.1. Параметры режима «массовой слежки», выведенные из-под проверки

Сразу несколько параметров режима «массовой слежки» оказались выведены ЕСПЧ из-под проверки на соответствие уже наработанным в практике Суда критериям, при-

[52] См. список организаций: *Big Brother Watch v. UK*. Appendix. P. 186.

[53] См.: *Big Brother Watch v. UK*. § 269.

[54] См.: *Centrum för Rättvisa v. Sweden*. § 112.

[55] См.: *Big Brother Watch v. UK*. § 315, 329; *Centrum för Rättvisa v. Sweden*. § 113.

[56] См.: *Big Brother Watch v. UK*. § 315, 329.

меняемым в рамках статьи 8 Конвенции, в качестве следствия признания допустимости массового перехвата данных *per se*. Причём в постановлении *Биг Бразер Вотч* Суд эксплицитно отметил не все, а только два таких изъятия, указав, что к данному типу слежки по определению не могут применяться ни критерий «обоснованного подозрения» в отношении лиц, чьи данные перехватываются, ни последующее уведомление о проводившейся операции[57].

Отказ от критерия «обоснованного подозрения» на самом деле является отказом от применения любого вида подозрения, и это явное отступление от собственной позиции, сформулированной в делах *Роман Захаров*, а также *Сабо и Висси*. А исключая требование об *ex post facto* уведомлении, ЕСПЧ пересмотрел свой подход, зафиксированный в первом касавшемся «массовой слежки» деле — *Вебер и Саравия*[58]. До принятия решения по делу *Биг Бразер Вотч* Суд признавал, что «последующее уведомление неразрывно связано с эффективностью мер судебной защиты и, соответственно, с существованием эффективных гарантий против злоупотребления властью по проведению мониторинга, поскольку, в принципе, у соответствующего индивида останется мало возможностей по обращению в суды, если только он не будет уведомлен о мерах, принятых без его согласия»; и что уведомление должно быть направлено так скоро после завершения слежки, как только это не «будет подрывать цели» применения данной меры[59]. Пусть Суд не исходил из абсолютного характера этого требования в *Вебер и Саравия*, но он явно был далёк от того, чтобы полностью от него отречься.

Другим исключением стало то, что ЕСПЧ отказался рассматривать в качестве необходимого предварительное получение судебного разрешения на проведение подобных операций. Сам Суд не преминул особо подчеркнуть, что это решение не вытекает из несовместимости данного требования с выводом о правомерности массовой слежки *per se*[60]. В отношении массового перехвата данных предварительная судебная санкция, по мнению ЕСПЧ, это не более чем «лучшая практика»[61]. Однако в этом признании сложно не заметить изрядную долю лукавства. Суд обосновывает такой шаг тем, что само по себе вынесение судебного решения, уполномочивающего на проведение подобной операции, не является гарантией от произвола. Аргументация ЕСПЧ при этом страдает нелогичностью, подсвечивая явную «натянутость» этого вывода. Суд приводит в качестве примера дело *Роман Захаров против России*[62], когда было установлено, что судьи при вынесении решений, разрешающих установление режима перехвата данных, из-за ограниченности судебного усмотрения не могли оценивать пропорциональность и необходимость введения этого режима, что низводило всю процедуру до уровня простой процессуальной формальности[63]. Схожие проблемы при проведении предварительного судебного контроля были установлены ЕСПЧ и по другим делам[64]. На этом основании Суд, казалось бы, верно подытоживает, что судебный контроль «сам по себе не является ни необходимым, ни достаточным для того, чтобы обеспечить соблюдение статьи 8 Конвенции»[65]. Однако это умозаключение нужно оценивать, принимая во внимание, какие ЕСПЧ выводит из него следствия. Вместо того чтобы прийти к выводу о толковании требования о предварительном судебном контроле как включающем в себя оценку его «качества», Суд решает отказаться от применения этого требования вообще[66]. В этой части ЕСПЧ соглашается с мнением Венецианской комиссии о том, что «независимый надзор может быть способен компенсировать отсутствие разрешения, выданного судом»[67]. Представляется, что за этой не выдерживающей критики линией рассуждений — как бы ни пытался откреститься от этого Суд — имплицитно стоит общий вывод о

[57] См.: *Big Brother Watch v. UK*. § 317.
[58] См.: *Weber and Saravia v. Germany*. § 135.
[59] См.: Ibid.; *Szabó and Vissy v. Hungary*. § 86.
[60] См.: *Big Brother Watch v. UK*. § 317.
[61] Ibid. § 318–320.
[62] См.: Ibid. § 319.
[63] См.: *Roman Zakharov v. Russia*. § 194; *Big Brother Watch v. UK*. § 319.
[64] См.: ECtHR. *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*. Application no. 62540/00. Judgment of 28 June 2007. § 85; *Mustafa Sezgin Tanrikulu v. Turkey*. Application no. 27473/06. Judgment of 18 July 2017. § 64.
[65] *Big Brother Watch v. UK*. § 320.
[66] См.: *Big Brother Watch v. UK*. Partly Concurring, Partly Dissenting Opinion of Judge Koskelo, Joined by Judge Turkovic. § 25.
[67] Ibid. § 318.

признании соответствия «массовой слежки» *per se* соответствующей Конвенции. ЕСПЧ, как это можно предположить, исходит из того, что предъявление требования о судебном санкционировании проведения подобных мероприятий не как формальности неразрывно сопряжено с необходимостью использования судами некоего стандарта оценки, который будет невозможен без оценки доказательств. В то же время отсутствие или недостаток конкретных доказательств (то есть предельно общий характер подозрений, которые могут лечь в основу установления «массовой слежки»), невозможность допуска судей к этим, даже если и имеющимся, то, скорее всего, засекреченным, данным, равно как и объём и количество дел, как раз и являются ключевыми характеристиками режима массового перехвата данных.

В рамках оценки предсказуемости национального законодательства ЕСПЧ также совершил несколько отступлений от наработанной схемы проверки, применяемой к целенаправленной слежке. В отношении природы правонарушений, которые служат поводом для инициирования мероприятий по массовому перехвату данных, Суд указал на то, что акцент должен смещаться на этап отбора полученной информации для проведения проверки[68]. Насколько ЕСПЧ ослабил это требование по отношению к проведению «массовой слежки», становится понятно, когда он признаёт, что общего упоминания в применимых правовых актах об угрозах «национальной безопасности» уже вполне достаточно для того, чтобы соответствовать этому требованию. То обстоятельство, что за этим термином может скрываться практически всё что угодно, ЕСПЧ оценил как его достоинство, а не недостаток[69]. В качестве аргумента Суд при этом апеллировал к тому, что понятие «национальная безопасность» «постоянно используется как в национальном, так и международном праве и представляет одну из легитимных целей, на которые ссылается пункт 2 статьи 8 [Конвенции]»[70]. ЕСПЧ не стал предъявлять сколь бы то ни было строгих требований и к формулированию круга правонарушений в актах о проведении конкретных операций. В самом постановлении по делу *Биг Бразер Вотч* в качестве примеров подобных формулировок приводятся такие фразы, как «материал, представляющий информацию о терроризме… включающий, но не ограниченный террористическими организациями, террористами, активно симпатизирующими лицами, планированием нападений, сбором средств»[71]. Суд ограничился указанием только на то, что использование более чётких выражений «было бы очень желательно»[72]. Представляется, что поразительная готовность ЕСПЧ довольствоваться таким уровнем абстракции может быть продиктована только изначально принятым решением о предельно широкой дискреции государств по использованию массового перехвата данных.

Оценка предсказуемости законодательной базы включает в себя и такой элемент, как возможность чётко установить круг лиц, в отношении которых будет применяться соответствующая мера. В отношении «массовой слежки» Суд сухо констатирует: «понятно, что эта категория является широкой»[73]. Разграничение сообщений на «внешние» (когда известно, что одна из сторон находится не на территории государства) и «внутренние» и исключение последних из-под режима перехвата[74] фигурируют в аргументации ЕСПЧ по данному вопросу только в связи с тем, что подобное ограничение было использовано в оцениваемом на соответствие Конвенции законодательстве Соединённого Королевства. Ещё одно ограничение Суд считает очевидным, отмечая, что, хотя «потенциально сообщения любого человека могут быть перехвачены», «*ясно*, что секретные службы не только не перехватывают все сообщения, но и не пользуются беспрепятственной дискрецией по перехвату любых сообщений по своему выбору»[75] (выделено мной. – *В.Р.*). В части пределов этой дискреции ЕСПЧ указывает на необходимость соблюдения национального законодательства, а также пропорциональность массового перехвата данных преследуемой цели[76]. Учитывая позицию Су-

[68] См.: *Big Brother Watch v. UK*. § 329.
[69] См.: Ibid. § 333, 332.
[70] Ibid. § 333.
[71] Ibid. § 342, 156.
[72] Ibid. § 342.
[73] Ibid. § 336.
[74] См.: Ibid. § 336, 337.
[75] Ibid. § 337.
[76] См.: Ibid.

да в отношении формулирования цели, становится понятно, что требование об определённости круга лиц, чьи данные могут быть перехвачены государством, фактически не предъявляется.

Всеохватывающий, не ограниченный конкретными целями характер режима «массовой слежки» получает отражение в том, что в постановлении *Биг Бразер Вотч и другие против Соединённого Королевства* ЕСПЧ отказывается применять ранее выведенное в решении по делу *Вебер и Саравия*[77] правило о том, что критерии поиска, применяемые к перехваченным данным, должны быть указаны в приказе о проведении операции. «Это с необходимостью подорвало и ограничило бы применение приказа, — указывает Суд в решении 2018 года, — и было бы в любом случае нереалистичным»[78]. Гарантией защиты от произвола, по мнению ЕСПЧ, должно быть то, что эти поисковые слова и так называемые «селекторы» должны быть предметом независимого надзора[79]. Отсутствие такого надзора как раз и является тем основанием, по которому ЕСПЧ устанавливает нарушение статьи 8 Конвенции[80].

Таким образом, получается, что, используя логический ход по признанию массовой слежки допустимой *per se*, ЕСПЧ ещё в бóльшей степени, чем это было в 2006 году в деле *Вебер и Саравия*, ограничивает действие предусмотренного в Конвенции права на уважение частной жизни.

3.2. Проверяемые на соответствие Конвенции параметры «массовой слежки»: где строгость, там и милость

Далее необходимо установить, действительно ли и в какой именно части ЕСПЧ применил строгий подход к оценке соответствия Конвенции правовой базы, регулирующей массовый перехват данных, за пределами того, что было изъято из-под этой проверки.

Начать следует с того, что Суд не вывел в постановлении *Биг Бразер Вотч* каких-либо новых критериев, которые должны применяться к режиму массовой слежки. Во-первых, он предсказуемо опирался на перечень из шести критериев, сформулированных в деле *Вебер и Саравия*, исключив из него первые два, к которым относятся природа правонарушений, которые могут служить основанием для выдачи приказа о перехвате сообщений, и определение категорий лиц, чьи сообщения могут перехватываться[81] (как уже указывалось, это было сделано в связи с признанием массовой слежки *per se* не нарушающей Конвенцию). Оставшиеся четыре критерия включали в себя: ограничение продолжительности перехвата данных; процедуру, которая должна использоваться для проверки, использования и хранения полученных данных; меры предосторожности, которые должны быть приняты при передаче данных другим сторонам; а также обстоятельства, при которых перехваченные данные должны быть стёрты или уничтожены[82]. Во-вторых, этот перечень был дополнен критериями, выведенными в деле *Роман Захаров против России*, среди которых: обеспечение надзора за применением мер по тайной слежке, введение процедуры уведомления, а также наличие средств правовой защиты[83].

Новеллой в подходе Суда, которую многие поспешили назвать победой в деле отстаивания права на частную жизнь[84], стало расширение в постановлении *Биг Бразер Вотч* круга информации, перехватывание которой может составлять посягательство на статью 8 Конвенции, с содержания сообщений до их метаданных[85]. Ключевые положения решения в этой части состоят в том, что Суд отказывается признавать «получение метаданных в меньшей степени покушающимися на права человека по сравнению с получением доступа к содержанию сообщений»[86] и подчёркивает, что «закономерности, которые будут выявлены, могут быть способны нарисовать интимную картину личности путём картографирования социальных сетей, отслеживания местоположения, а также истории использования интернет-браузеров, выявления паттер-

[77] См.: *Weber and Saravia v. Germany*. § 32.
[78] *Big Brother Watch v. UK*. § 340.
[79] См.: Ibid. § 340.
[80] См.: Ibid. § 347, 387.
[81] См.: *Big Brother Watch v. UK*. § 424.
[82] См.: Ibid.
[83] См.: *Roman Zakharov v. Russia*. § 238.
[84] См., например: *Milanovic M*. ECtHR Judgment in Big Brother Watch v. UK.
[85] В тексте решения ЕСПЧ использует термин “related communications data”.
[86] *Big Brother Watch v. UK*. § 356.

нов коммуникаций, равно как и инсайда о тех, с кем происходило общение»[87]. ЕСПЧ, действительно, впервые распространил защиту Конвенции на этот тип данных, однако в данном, несомненно прогрессивном, шаге есть одно «но», которое серьёзно нивелирует это свершение. Дело в том, что, повторив заветные фразы, за появление которых в судебных решениях так давно боролись правозащитные организации, ЕСПЧ не уравнял режимы проверки перехвата содержания сообщений и их метаданных. Суд не вышел на применимость шести минимальных критериев, выведенных в деле *Вебер и Саравия*, к метаданным, указав только на то, что изъятие этих данных из круга информации, к которым применяются гарантии, предусмотренные национальным законодательством, не является оправданным[88]. Отсюда, в деле борьбы за признание перехвата метаданных таким же, если не бóльшим, вторжением в частную жизнь, как и получение доступа к содержанию сообщений, ещё рано ставить точку.

Появление другой новеллы в постановлении по делу *Биг Бразер Вотч* было связано не с изменением уже применявшегося ранее подхода, а обусловлено тем, что перед Судом впервые был поставлен вопрос о соответствии Конвенции режима получения перехваченной информации от иностранных спецслужб[89]. Исключив из области проверки стадию перехвата данных по причине отсутствия у ответчика юрисдикции и невозможности вменить ему эти действия[90], ЕСПЧ оценивал получение Соединённым Королевством данных, их последующее хранение, проверку и использование[91]. Обоснованность такого исключения вызывает вопросы. Суд отмечает, что непосредственно перехват данных может осуществляться в том числе по запросу ответчика[92]. Не должно ли это влечь возникновение международной ответственности у государства, которое направляет такой запрос? ЕСПЧ, ссылаясь на Статьи об ответственности государств[93] (*далее* — Статьи), однозначно утверждает, что нет, так как эта ситуация не подпадает ни под один из описанных в них случаев. Представляется, из всех предусмотренных в этих Статьях вариантов можно было бы рассматривать осуществление руководства и контроля над другим государством в совершении последним международно-противоправного деяния, если бы не очень высокая планка, которая предъявляется при установлении наличия такого «руководства и контроля»: «реальное руководство оперативного плана»[94]. Таким образом, Суд оказывается прав: действия по перехвату, совершённые другим государством, нельзя вменить государству-ответчику. Решением могло бы быть рассмотрение действий обоих государств через призму «совместной ответственности», если бы эта концепция имела нормативный характер[95]. В любом случае проблемой являлось бы и установление осуществления «юрисдикции» по статье 1 Конвенции[96]. Соответственно, как право международной ответственности, так и сфера применения Конвенции не позволяют выйти на оценку перехвата данных, оставляя серьёзный пробел в защите прав человека, которым вполне могут пользоваться или уже воспользовались государства — участники Конвенции.

Однако исключение этапа получения данных не является единственной особенностью проверки схемы сотрудничества спецслужб на соблюдение статьи 8 Конвенции. При проверке использования данных, полученных от иностранных спецслужб, ЕСПЧ, казалось бы, применяет выведенные в делах *Вебер и Саравия* и *Роман Захаров* критерии. Эксплицитно Суд указывает на некоторое ослабление требований к описанию обстоятельств, при которых может быть направлен запрос о

[87] *Big Brother Watch v. UK*. § 356.
[88] См.: Ibid. § 352–357.
[89] См.: Ibid. 416.
[90] См.: Ibid. 420.
[91] См.: Ibid. 421.
[92] См.: Ibid. § 417, 420.
[93] См.: Статьи об ответственности государств за международно-противоправные деяния, приняты резолюцией Генеральной Ассамблеи ООН A/RES/56/83 «Ответственность государств за международно-противоправные деяния». Статья 8. URL: http://www.un.org/ru/documents/decl_conv/conventions/pdf/responsibility.pdf (дата обращения: 03.12.2018).
[94] *Crawford J.* The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries. Cambridge ; New York : Cambridge University Press, 2002. P. 154; Draft articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries 2001 // Yearbook of the International Law Commission. 2001. Vol. II. Part 2. P. 26–116, 68–69.
[95] См.: *Nollkaemper A., Jacobs D.* Shared Responsibility in International Law: A Conceptual Framework // Michigan Journal of International Law. Vol. 34. 2013. No. 2. P. 359–438, 363.
[96] См.: *Milanovic M.* Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age // Harvard International Law Journal. Vol. 56. 2015. No. 1. P. 81–146, 124–129.

предоставлении перехваченного материала[97]. Однако при этом ЕСПЧ вообще не применяет критерий, связанный с длительностью и, соответственно, необходимостью прекращения перехвата данных. Помимо этого, обращает на себя внимание и то, что при анализе процедуры проверки перехваченных данных и, по сути, по второму кругу оценивая те же нормы британского законодательства, которые уже были предметом рассмотрения в этом постановлении, Суд решил не повторять, что имело место нарушение, связанное с отсутствием надзора за выбором сообщений на стадии фильтрации и их отбора для проверки аналитиком[98]. Здесь можно лишь гадать, является ли такое упущение сознательным или же оно было допущено по ошибке.

В нескольких аспектах постановления по делу *Биг Бразер Вотч* можно разглядеть не ужесточение, а ослабление ЕСПЧ уже занятой ранее позиции. Во-первых, ЕСПЧ решил снизить ранее выведенную планку требований к надзору за проведением операций по массовому перехвату данных. В 2015 году в деле *Роман Захаров против России* Суд сформулировал, что, если компетенцией уполномочивать на установление слежки наделён не судебный орган, это всё ещё может быть совместимо с Конвенцией, если этот орган «достаточно независим от исполнительной власти»[99]. В постановлении по делу *Биг Бразер Вотч* ЕСПЧ явно идёт на попятную, указывая, что требовал этого «в общем», в частности же нужно принимать во внимание «непосредственное использование системы перехвата в целом, включая сдержки и противовесы осуществления власти, существование (или отсутствие) каких-либо доказательств реальных злоупотреблений... таких как уполномочивание на проведение таких операций на беспорядочной и нерегулярной основе или без надлежащего рассмотрения»[100].

Во-вторых, несмотря на признание допустимым предельно общего формулирования целей, ради которых устанавливается режим массового перехвата данных, в предыдущих делах Суд требовал, чтобы принимаемые государством меры были необходимы для их достижения. В постановлении *Биг Бразер Вотч*, анализируя британское законодательство, ЕСПЧ выявил, что в качестве обстоятельства, при котором перехваченные данные могут быть переданы или скопированы, указан случай, когда эти действия, «вероятно, могут стать необходимыми» (англ.: "likely to become necessary") для достижения «одобренной цели»[101]. Это, однако, не вылилось в признание нарушения из-за того, что ЕСПЧ принял во внимание, что круг лиц, которые могут воспользоваться этой возможностью, ограничен имеющими необходимый уровень допуска, и ограничился на сей счёт лишь рекомендацией[102].

4. Новый подход Европейского Суда по правам человека к массовой слежке как отражение консенсуса «Больших братьев»?

Сам Суд в постановлении по делу *Биг Бразер Вотч* уделил очень мало внимания обоснованию своего стратегического выбора в пользу легитимности массовой слежки как таковой, представив следующие аргументы. Во-первых, не отрицая произошедший качественный скачок в информационных технологиях, ЕСПЧ тем не менее сделал упор на то, что им воспользовались «террористы и преступники», которым это помогает «избежать обнаружения в Интернете»[103]. Во-вторых, введение режима массового перехвата данных Суд обосновал непредсказуемостью путей, по которым передаются электронные сообщения[104]. В-третьих, рассуждая об эффективности этой меры и выполнении ею упреждающей функции, ЕСПЧ указал на отсутствие альтернатив, которые могли бы заменить режим массового перехвата данных[105].

Эти аргументы представляются явно односторонними: учитывая возросшие возможности по использованию технологий, ЕСПЧ замечает только «террористов и преступников», предпочитая умолчать об увеличивающихся по экспоненте аппетитах государств по сбору и анализу информации о гражданах. Всего десять лет назад эти желания техноло-

[97] См.: *Big Brother Watch v. UK*. § 424, 428–430.
[98] См.: Ibid. § 387.
[99] *Roman Zakharov v. Russia*. § 258.
[100] *Big Brother Watch v. UK*. § 377.
[101] Ibid. § 368.
[102] См.: Ibid.
[103] Ibid. § 314.
[104] См.: Ibid.
[105] См.: Ibid. § 384.

гически сдерживались отсутствием или неэффективностью систем по хранению и обработке больших данных. Наконец, апеллируя к отсутствию альтернатив, Суд не рассматривает меры по установлению целенаправленной слежки. Частое использование ЕСПЧ при обосновании своего выбора слов «понятно» и «ясно», заставляет задуматься о том, что в действительности имеется в виду: здравый смысл, эффективность применения мер, технические возможности или всё в совокупности? В большинстве же случаев это всего лишь слегка замаскированная обратная отсылка к постулату о том, что массовый перехват данных *per se* не является нарушением Конвенции.

Что же в действительности могло стоять за решением Суда? Если исходить из принципиальной способности международного права прав человека и, в частности, Конвенции о защите прав человека и основных свобод, несмотря на различные ограничения сферы её применения, выступить в качестве инструмента, который может быть использован для запрета «массовой слежки» со стороны государств-участников, то необходимо разобраться с тем, почему ЕСПЧ не решился взять на себя смелость использовать заложенную в конструкцию статьи 8 возможность объявить не основанную на наличии обоснованного подозрения слежку нарушающей Конвенцию. Какие *политические основания* оказали бóльшее влияние при применении Судом метода «балансирования», предопределив трактовку того, что является «необходимым в демократическом обществе»[106]?

Начиная с 2001 года как общественное мнение, так и отношение Совета Европы и Европейского Союза к допустимости «массовой слежки» неоднократно менялось[107]. Маятник снова пришёл в движение, следуя за сделанными в 2013 году разоблачениями Э. Сноудена: открыв глаза на масштабность программ электронной слежки, они катализировали как политические, так и юридические попытки привлечь власть к ответственности и оформили массовый запрос на то, чтобы если не запретить, то существенно сократить и ограничить возможности по перехвату данных. Однако в связи с тем, что с 2015 года по Европе прокатилась волна террористических актов (Париж, Брюссель, Ницца, Берлин, Манчестер, Лондон, Барселона), маятник общественного мнения качнулся в другую сторону, чем не преминули воспользоваться многие государства, чтобы, приняв соответствующее законодательство, урегулировать и тем самым, с одной стороны, ограничить, а с другой — легализовать массовый перехват данных на национальном уровне.

К примеру, во Франции практически сразу после терактов в Париже 30 ноября 2015 года был принят Закон о мерах по слежке за международными электронными коммуникациями[108], который позволяет перехватывать все сообщения, направленные за границу или полученные за границей[109], и хранить контент сообщений один год, а метаданные — шесть лет[110]. В ФРГ 23 декабря 2016 года был принят Закон о перехвате зарубежных сообщений Федеральной разведывательной службой[111], в котором регулируется слежка за гражданами иностранных государств[112]. В 2016 году изменения в швейцарское законодательство, значительно расширяющие возможности по установлению массовой слежки, были вынесены на референдум и получили одобрение со стороны 65,5 % его участников[113]. В этом же году были внесены изменения в польский Закон о полиции и некоторые

[106] См.: *Koskenniemi M.* The Politics of International Law. Oxford ; Portland, OR : Hart Publishing, 2011. P. 146.

[107] См.: European Parliament. Resolution on the First Report on the Implementation of the Data Protection Directive (95/46/EC) (COM(2003) 265 — C5-0375/2003 — 2003/2153(INI)). URL: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A5-2004-0104+0+DOC+XML+V0//EN&language=en (дата обращения: 16.11.2018); European Council. Declaration on Combating Terrorism of 25 March 2004, § 11. URL: https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/79637.pdf (дата обращения: 16.11.2018). См. также: *Maras M.-H.* The Social Consequences of a Mass Surveillance Measure: What Happens When We Become the "Others"? // International Journal of Law, Crime and Justice. Vol. 40. 2012. No. 2. P. 65—81, 65—66.

[108] См.: Loi n°2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales. URL: https://www.legifrance.gouv.fr/eli/loi/2015/11/30/DEFX1521757L/jo/texte (дата обращения: 16.11.2018).

[109] См.: Ibid. Article 1.

[110] См.: Ibid.

[111] См.: Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes vom 23. Dezember 2016 // Bundesgesetzblatt. 2016. Teil I. Nr. 67. S. 3346—3353.

[112] См. подр.: *Wetzling Th., Simon S.* Eine kritische Würdigung der BND-Reform. URL: https://verfassungsblog.de/eine-kritische-wuerdigung-der-bnd-reform/ (дата обращения: 16.11.2018).

[113] См.: URL: https://www.theguardian.com/world/2016/sep/25/switzerland-votes-in-favour-of-greater-surveillance (дата обращения: 16.11.2018). См.: Bundesgesetz betreffend die Über-

другие акты, регулирующие использование тайной слежки[114].

Таким образом, принимая постановления по делам *Центрум фёр Рэттвиса* и *Биг Бразер Вотч*, ЕСПЧ, изменив свой собственный подход, пошёл в фарватере развития законодательства и подходов европейских государств. Подтверждением тому может служить то, что решение по делу *Биг Бразер Вотч* изобилует ссылками на доклад Венецианской комиссии «О демократическом надзоре за службами, занимающимися радиоэлектронной разведкой»[115]. В частности, вывод ЕСПЧ о допустимости массовой слежки *per se* базируется на позиции Венецианской комиссии, признающей существенным вторжением в право на защиту частной жизни не сбор, а доступ и последующую работу с перехваченными данными[116]. Важно подчеркнуть, что комиссия предварила этот вывод ссылкой на существующую «европейскую перспективу»[117]. Хотя в докладе это понятие нигде не раскрывается, можно судить о том, что члены Венецианской комиссии исходили из некоего общего подхода, складывающегося из суммирования позиций европейских государств, а не практики ЕСПЧ и Суда ЕС. Такое заключение можно сделать на том основании, что в докладе вывод о необходимости переноса акцента на доступ и последующую работу с данными не сопряжён с дифференциацией целей установления слежки, в то время как на момент принятия доклада ЕСПЧ и Суд ЕС требовали от государств, чтобы тайная слежка в рамках борьбы с преступлениями, включая сбор данных, проходила только на основании обоснованного подозрения[118].

Конечно, ЕСПЧ не мог не учитывать и крайне скептического отношения европейских государств к исполнению решений, связанных с ограничением возможностей по использованию массового перехвата данных. К примеру, большинство государств, входящих в ЕС, либо не исполнили, либо не в полной мере исполнили решение Суда ЕС по делу *Диджитл Райтс Ирландия*[119]. Кроме того, общей тенденцией является то, что в государствах, законодательство которых претерпело изменения, перемены были запущены не органами власти, а стали результатом судебных процессов, инициированных неправительственными организациями[120]. В Российской Федерации и в Венгрии так и не были приняты меры общего характера по исполнению постановлений по делам *Роман Захаров* и *Сабо и Висси*[121]. Можно предположить, что для ЕСПЧ, пусть не «авторитет», а «власть» которого серьёзно подтачиваются так называемым «стратегическим неисполнением» его решений рядом государств-членов[122], способность и готовность прямо пойти против подхода, сложившегося на национальном уровне, существенно ограничены в силу действия институционального инстинкта самосохранения.

5. На пути к всеобщему «паноптикуму»...

Многие авторы, исследовавшие применимость международного права прав человека

wachung des Post- und Fernmeldeverkehrs vom 18. März 2016 (stand am 1. März 2018). URL: https://www.admin.ch/opc/de/classified-compilation/20122728/index.html (дата обращения: 16.11.2018).

[114] См.: European Commission for Democracy through Law (Venice Commission). Opinion on the Act of 15 January 2016 Amending the Police Act and Certain Other Acts of 10–11 June 2016. URL: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)012-e (дата обращения: 16.11.2018).

[115] См.: Venice Commission. Report of 2015.

[116] См.: Ibid. § 60.

[117] Ibid.

[118] См.: ECtHR: *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*. Application no. 62540/00. Judgment of 28 June 2007. § 79, 80; *Iordachi and Others v. Moldova*. Application no. 25198/02. Judgment of 10 February 2009. § 51; *Digital Rights Ireland*. § 57.

[119] См.: Privacy International. National Data Retention Laws since the CJEU's Tele-2/Watson Judgment. September 2017. P. 12. URL: https://privacyinternational.org/sites/default/files/2017-12/Data%20Retention_2017.pdf (дата обращения: 16.11.2018).

[120] См.: Ibid. P. 13.

[121] См.: UN Human Rights Committee, Concluding Observations on the Sixth Periodic Report of Hungary of 29 March 2018. CCPR/C/HUN/CO/6. § 43. URL: https://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR/C/HUN/CO/6&Lang=En (дата обращения: 16.11.2018); Комитет Министров Совета Европы. Дело «Роман Захаров против Российской Федерации» (Жалоба № 47143/06). Решение от 5–7 декабря 2017 года. 1302-е заседание, CM/Del/Dec(2017)1302/H46-26. URL: https://rm.coe.int/roman-zakharov-decision-1302-ru/16807bfa5f (дата обращения: 16.11.2018).

[122] См.: *Madsen M. R.* The Challenging Authority of the European Court of Human Rights: from Cold War Legal Diplomacy to the Brighton Declaration and Backlash // Law And Contemporary Problems. Vol. 79. 2016. No. 1. P. 141–178, 175. См. также: *De Londras F., Dzehtsiarou K.* Mission Impossible? Addressing Non-Execution Through Infringement Proceedings in the European Court of Human Rights // International and Comparative Law Quarterly. Vol. 66. 2017. No. 2. P. 467–490.

в «цифровую эру» как до, так и после вынесения ЕСПЧ постановления по делу *Биг Бразер Вотч*, исходят из того, что электронная «массовая слежка» *per se* не является нарушением международно-правовых обязательств государств в сфере защиты права на частную жизнь и свободы выражения[123]. Однако, маргинализируя идею о возможности признания нелегальности использования «массовой слежки» в свете прав человека как, пользуясь известной дихотомией М. Коскенниеми, исключительно «утопическую», мы можем не заметить постепенной трансформации государств в дистопии.

ЕСПЧ, конечно, не является единственным органом, который обладает компетенцией по проверке соблюдения прав человека, однако нельзя исключать, что его постановления по делам *Центрум фёр Раттвиса* и *Биг Бразер Вотч* в той или иной степени окажут влияние на позицию Суда ЕС, и он тоже сочтёт, что избранный ранее путь, возможно, был «слишком прогрессивным». Позиция Комитета ООН по правам человека, а равно специальных докладчиков ООН, при всём своём критическом отношении к «массовой слежке», нивелируется отсутствием обязательной силы принимаемых решений или озвучиваемых подходов. Кроме того, давно ожидаемое новое Замечание общего порядка к статье 17 Международного пакта о гражданских и политических правах до сих пор так и не принято[124]. Наконец, защита, предоставляемая гражданам демократических государств их конституциями, может оказаться недостаточной. Ярким примером тому может служить вынесенное в 2016 году Федеральным конституционным судом Германии решение, в котором он пришёл к выводу, что отказ в раскрытии специальной парламентской комиссии «селекторов» и поисковых слов, применяемых при массовом сборе данных в рамках сотрудничества германских и американских спецслужб (BND и NSA), когда, возможно, перехватывались и сообщения граждан ФРГ, не является нарушением Основного закона[125]. В основу решения суд положил постулат о том, что интерес в поддержании способности правительства осуществлять внешнюю политику и политику в области безопасности «перевешивает» право парламентской комиссии на ознакомление со списками «селекторов»[126]. Кроме того, даже если программы по «массовой слежке» действительно исключают граждан своего государства, конституционная защита может оказаться иллюзорной, потому как нельзя забывать, что «все мы — иностранцы»[127]: запрет на массовую слежку за собственными гражданами может быть с лёгкостью обойдён путём сотрудничества со спецслужбами других государств.

Анализируя постановление ЕСПЧ по делу *Биг Бразер Вотч*, сложно не заметить, как с «широко закрытыми глазами» общество движется ко всеобщему «паноптикуму», точь-в-точь реализуя описанный Мишелем Фуко сценарий. В частности, в своём труде «Надзирать и наказывать. Рождение тюрьмы», изданном в 1975 году, он очень чётко охарактеризовал роль государства в слежке за своими гражданами: «Надо раз и навсегда перестать описывать проявления власти в отрицательных терминах: она, мол, “исключает”, “подавляет”, “цензурует”, “извлекает”, “маскирует”, “скрывает”. На самом деле, власть производит. Она производит реальность; она производит области объектов и ритуалы истины. Индивид и знание, которое можно получить об индивиде, принадлежат к её продукции»[128]. Решение ЕСПЧ, когда, предпочтя принципиальности эффективность, он снизил планку предъявляемых к государствам

[123] См., например: *Lubin A.* “We Only Spy on Foreigners”: The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance // Chicago Journal of International Law. Vol. 18. 2018. No. 2. P. 502–552, 545–546; *Milanovic M.* Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age. P. 82, 132; *Margulies P.* The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism // Fordham Law Review. Vol. 82. 2014. No. 5. P. 2137–2167, 2166; *Georgieva I.* The Right to Privacy under Fire — Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR // Utrecht Journal of International and European Law. Vol. 31. 2015. No. 80. P. 104–130, 128; *Verbruggen F.*, *Royer S.*, *Severijns H.* Op. cit.

[124] См.: *Joyce D.* Privacy in the Digital Era: Human Rights Online? // Melbourne Journal of International Law. Vol. 16. 2015. No. 1. P. 270–285, 276.

[125] См.: Bundesverfassungsgericht. Beschluss des Zweiten Senats vom 13. Oktober 2016. 2 BvE 2/15. URL: http://www.bverfg.de/e/es20161013_2bve000215.html (дата обращения: 16.11.2018).

[126] См.: Ibid. § 5 (Leitsätze).

[127] *Cole D.* We Are All Foreigners: NSA Spying and the Rights of Others // Just Security Blog. 2013. 29 October. URL: https://www.justsecurity.org/2668/foreigners-nsa-spying-rights/ (дата обращения: 16.11.2018).

[128] *Фуко М.* Надзирать и наказывать. Рождение тюрьмы / пер. с фр. В. Наумова ; под ред. И. Борисовой. М. : Ad Marginem, 1999. С. 284.

требований по защите права на частную жизнь, вполне может оказаться фатальным.

Библиографическое описание:
Русинова В. Легализация «массовой слежки» Европейским Судом по правам человека: что стоит за постановлением по делу *Биг Бразер Вотч и другие против Соединённого Королевства*? // Международное правосудие. 2018. № 4 (28). С. 3–20.

Legalization of "mass surveillance" by the European Court of Human Rights: what stands behind the judgment in the case of *Big Brother Watch and Others v. the United Kingdom*?

Vera Rusinova

Doctor of Sciences in Law, Professor, Faculty of Law, Higher School of Economics, Moscow, Russia (e-mail: vrusinova@hse.ru).

Abstract

On September 13, 2018, the European Court of Human Rights rendered a judgment in the case of *Big Brother Watch and Others v. the United Kingdom*, in which it examined whether the legal acts of the UK on the mass interception of communications and its meta-data, as well as the intelligence sharing regime with foreign intelligence agencies, corresponds to the Convention on the Protection of Human Rights and Fundamental Freedoms. Having used an approach under which "while States enjoy a wide margin of appreciation in deciding what type of interception regime is necessary to protect national security, the discretion afforded to them in operating an interception regime must necessarily be narrower," the Court thereby legalized the use of bulk interception of communications and meta-data. Assessing what content stands behind the acceptance of mass surveillance as not violating the Convention *per se*, this article demonstrates that the court, by acting both explicitly and implicitly, has exempted a number of key issues of these measures from the test on "legality", "necessity in democratic society", and "proportionality", and has also significantly lowered the threshold of requirements in respect to other components of the bulk surveillance regime. This is an obvious reversal from a sufficiently progressive approach to the protection of the right for respect of private life and personal data against the background of ever-growing appetite of states for mass collection of data, which started to crystallize few years ago in jurisprudence of the ECHR and the Court of Justice of the EU. The article concludes with reflections on the political grounds that could have influenced the ECtHR's application of the balancing method and predetermined its position on what is "necessary in a democratic society".

Keywords

right to respect for private life; privacy; mass surveillance; meta-data; European Court of Human Rights; Court of Justice of the European Union.

Citation

Rusinova V. (2018) Legalizatsiya "massovoy slezhki" Evropeyskim Sudom po pravam cheloveka: chto stoit za postanovleniem po delu *Big Brother Watch and Others v. the United Kingdom*? [Legalization of "mass surveillance" by the European Court of Human Rights: what stands behind the judgment in the case *of Big Brother Watch and Others v. the United Kingdom*?]. *Mezhdunarodnoe pravosudie*, vol. 8, no. 4, pp. 3–20. (In Russian).

References

Crawford J. (2002) *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries*, Cambridge; New York: Cambridge University Press.

De Londras F., Dzehtsiarou K. (2017) Mission Impossible? Addressing Non-Execution Through Infringement Proceedings in the European Court of Human Rights. International and Comparative Law Quarterly, vol. 66, no. 2. pp. 467–490.

Fuko M. (1999) Nadzirat'i nakazyvat'. Rozhdenie tyur'my [Oversee and punish. The birth of the prison], V. Naumov (transl.), I. Borisova (ed.), Moscow: Ad Marginem.

Georgieva I. (2015) The Right to Privacy under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR. *Utrecht Journal of International and European Law*, vol. 31, no. 80, pp. 104–130.

Golubok S. (2015) Roman Zakharov v. Russia: Big Brother Under Control? *Journal for Constitutionalism and Human Rights*, no. 3–4 (8). pp. 20–26.

Joyce D. (2015) Privacy in the Digital Era: Human Rights Online? *Melbourne Journal of International Law*, vol. 16, no. 1, pp. 270–285.

Koskenniemi M. (2011) *The Politics of International Law*, Oxford; Portland, OR: Hart Publishing.

Lubin A. (2018) "We Only Spy on Foreigners": The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance. *Chicago Journal of International Law*, vol. 18, no. 2. pp. 502–552.

Madsen M. R. (2016) The Challenging Authority of the European Court of Human Rights: from Cold War Legal Diplomacy to the Brighton Declaration and Backlash. *Law And Contemporary Problems*, vol. 79, no. 1, pp. 141–178.

Maras M.-H. (2012) The Social Consequences of a Mass Surveillance Measure: What Happens When We Become the 'Others'? *International Journal of Law, Crime and Justice*, vol. 40, no. 2, pp. 65–81.

Margulies P. (2014) The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism. *Fordham Law Review*, vol. 82, no. 5, pp. 2137–2167.

Milanovic M. (2015) Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age. *Harvard International Law Journal*, vol. 56, no. 1, pp. 81–146.

Nollkaemper A., Jacobs D. (2013) Shared Responsibility in International Law: A Conceptual Framework. *Michigan Journal of International Law*, vol. 34, no. 2, pp. 359–438.

Pásztor E. (2017) Secret Intelligence Gathering – a Low Threshold Still Too High to Reach. *ELTE Law Journal*, no. 1, pp. 99–112.